Práctica 4 SWAP

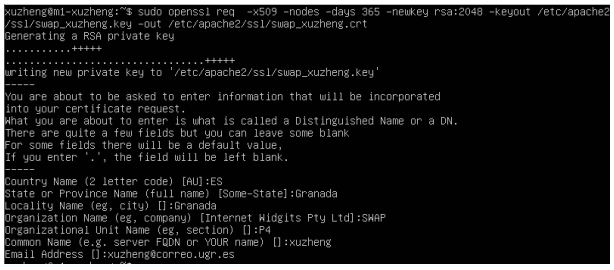
XuSheng Zheng

Índice

1. Certificado autoafirmado SSL

Empezamos habilitando el módulo SSL de Apache y creando el directorio para ubicar los certificados:

Ahora creamos los certificados con los siguientes datos:



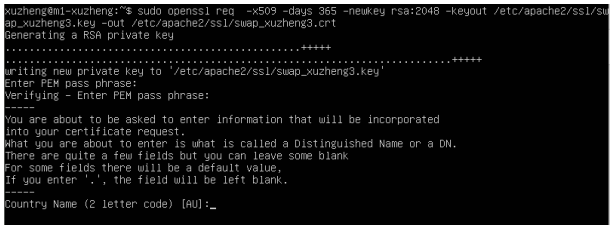
1.1. Opciones avanzadas

De las opciones introducidas anteriormente, podemos prescindir de **nodes** para añadir una contraseña a la clave. Además, tenemos las siguientes opciones que pueden ser interesantes:

- **-config filename**: permite especificar un archivo de configuración para la creación de los certificados.
- **-subj arg**: permite especificar datos para la creación del certificado. El argumento debe ser de la forma **/type0=value0/type1=value1/type2=....**. Al introducir esta opción no nos pedirá los datos como habíamos hecho.
- **-addext ext**: permite añadir una extensión de x509 en el certificado generado.

Como ejemplo creamos el siguiente certificado:

Podemos ver que nos pide la contraseña para generar los certificados. Si eliminamos la opción **-subj** podemos ver que aparte de pedirnos la contraseña nos pide también el resto de informaciones:



2. Apache con certificado SSL

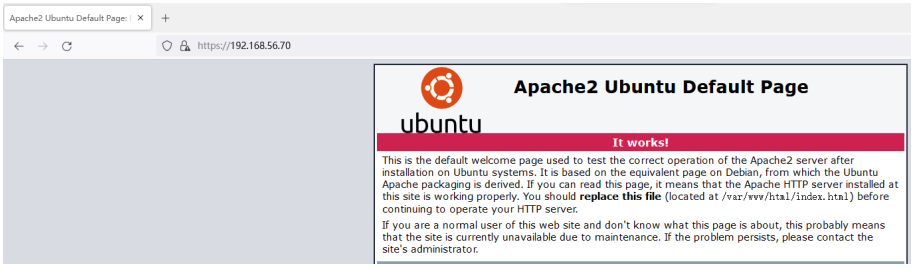
Editamos el archivo de configuración */etc/apache2/sites-available/default-ssl.conf*:

```
#   Enable/Disable SSL for this virtual host.
SSLEngine on

SSLCertificateFile /etc/apache2/ssl/swap_xuzheng.crt
SSLCertificateKeyFile /etc/apache2/ssl/swap_xuzheng.key

#   A self-signed (snakeoil) certificate can be created by installing
#   the ssl-cert package. See
#   /usr/share/doc/apache2/README.Debian.gz for more info.
#   If both key and certificate are stored in the same file, only the
#   SSLCertificateFile directive is needed.
#SSLCertificateFile    /etc/ssl/certs/ssl-cert-snakeoil.pem
#SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key

#   Server Certificate Chain:
#   Point SSLCertificateChainFile at a file containing the
#   concatenation of PEM encoded CA certificates which form the
#   certificate chain for the server certificate. Alternatively
#   the referenced file can be the same as SSLCertificateFile
#   when the CA certificates are directly appended to the server
#   certificate for convinience.
#SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt
```

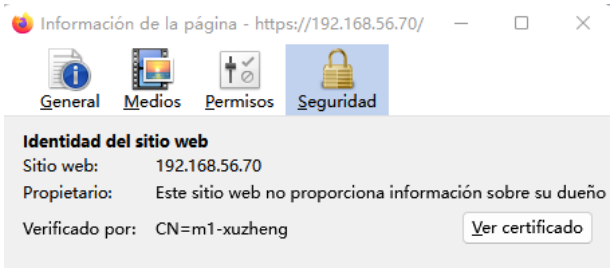
Activamos **default-ssl** y reiniciamos Apache:

```
xuzheng@m1-xuzheng:~$ sudo a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
xuzheng@m1-xuzheng:~$ sudo service apache2 reload
```

Para comprobar que se ha instalado correctamente el certificado accedemos desde el navegador del anfitrión:



Accedemos al certificado desde el candado con exclamación a la izquierda de la URL:



Certificado

xuzheng

Nombre del asunto

País	ES
Estado/Provincia	Granada
Localidad	Granada
Organización	SWAP
Unidad organizativa	P4
Nombre común	xuzheng
Dirección de correo electrónico	xuzheng@correo.ugr.es

Nombre del emisor

País	ES
Estado/Provincia	Granada
Localidad	Granada
Organización	SWAP
Unidad organizativa	P4
Nombre común	xuzheng
Dirección de correo electrónico	xuzheng@correo.ugr.es

Validez

No antes	Fri, 21 Apr 2023 15:56:27 GMT
No después	Sat, 20 Apr 2024 15:56:27 GMT

3. Bibliografía

- https://linux.die.net/man/1/scp
- https://linux.die.net/man/1/tar
- https://serverfault.com/questions/141773/what-is-archive-mode-in-rsync
- https://ss64.com/bash/rsync.html
- https://linux.die.net/man/1/rsync
- https://serverfault.com/questions/123629/run-task-every-90-minutes-with-cron